REMARKS

The Office Action mailed March 22, 2006 has been reviewed and carefully considered. No new matter has been added.

Claim 1 has been amended. New Claims 6 and 7 have been added. Claims 1-7 are pending.

Claims 1-5 stand rejected under 35 U.S.C. §102(b) as being anticipated by SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 (hereinafter "Stallings").

Claim 1 has been amended to better clarify the Applicants' invention. As the words of Claim 1 have been essentially re-arranged, it is respectfully asserted that no new matter has been added.

It is respectfully asserted that Stallings does not teach or suggest "utilizing a Diffie-Hellman key exchange protocol by the SNMP manager and the SNMP agent to enter an initial privacy key and an initial authentication key into the SNMPv3 device", as recited in Claim 1.

In contrast to the preceding limitations of Claim 1, Stallings simply generates keys from a password, and does not disclose or even remotely suggest the use of the Diffie-Hellman key exchange to generate the keys.

In further detail, Stallings discloses "a requirement of the use of the authentication and privacy services of SNMPv3 is that, for any communication between a principal on a non-authoritative engine and a remote authoritative engine, a secret authentication key and a secret privacy key must be shared. These keys enable a user at a non-authoritative (typically a management system) to employ authentication and privacy with remote authoritative systems that the user managers (typically, agent systems). RFC 2274 provides guidelines for the creation, update, and management of these keys" (Stallings, p. 11, col. 2, lines 54-63).

Stallings further discloses "These keys are not stored in a MIB and are not accessible via SNMP" (Stallings, p. 11, col. 2, lines 60-61).

Moreover, Stallings discloses "A user requires a 16-octet privacy key and an authentication key of length either 16 or 20 octets. For keys owned by human users, it is desirable that the user be able to employ a human-readable password rather than a bit-string key. Accordingly, RFC 2274 defines an algorithm for mapping from the user password to a 16- or 20-octet key" (Stallings, p. 12, col. 1, lines 29-34).

Stallings continues, at page 12, column 1, lines 38-48:

Password to key generation is performed as follows:

1. Take the user's password as input and produce a string of length 2^{20} octets (1,048,576 octets) by repeating the password value as many times as necessary, truncating the last value of necessary, to form the string digest0. For example, an eight-character password (23 octets) would be concatenated with itself 217 times to form digest0.

2. If a 16-octet key is desired, take the MD5 hash of digest0 to form digest1. If a 20-octet key is desired, take the SHA-1 hash of digest0 to form digest1. The output is the user's key.

Thus, the approach of Stallings, as also shown in FIG. 7 thereof, expands a password string of user password, takes the hash of the expanded password string to obtain a user key, and takes the hash of the user key and remote engineID to obtain a localized key.

However, in contrast to the express limitations of Claim 1, Stallings makes no mention of computing a shared secret using the Diffie-Hellman key exchange protocol. Advantageously, "it is to be appreciated that the Diffie-Hellman key exchange ensures that both the agent and the manager compute the same 16 character password without revealing it" (Applicants' specification, p. 8, lines 21-23).

Accordingly, Stallings is also silent with respect to the generation of a random number by the both the SNMP manager and the SNMP agent, and is further silent in the use of the random number in the Diffie-Hellman key exchange protocol as essentially recited in Claim 1.

Moreover, Stallings is additionally silent with respect to the reading of the public value of the SNMP agent by the SNMP manager through a SNMP request using an initial valid user having access to the public value of the SNMP agent, the public value for use in the Diffie-Hellman key exchange as essentially recited in Claim 1.

A reference cited against a claim under 35 U.S.C. §102 must disclose each and every limitation of the rejected claim. Accordingly, independent Claim 1 is patentably distinct and non-obvious over the cited reference for at least the reasons set forth above.

Claims 2-5 depend from Claim 1 or a claim which itself is dependent from Claim 1 and, thus, includes all the elements of Claim 1. Accordingly, Claims 2-5 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 1.

Accordingly, reconsideration of the rejections is respectfully requested.

Moreover, new Claims 6 and 7 have been added. Support for Claims 6 and 7 may be found at page 6, lines 16-19 and page 7, lines 4-10 of the Applications' specification.

Claims 6 and 7 depend from Claim 1 and, thus, includes all the elements of Claim 1. Accordingly, Claims 6 and 7 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 1.

Moreover, Claims 6 and 7 include patentable subject matter in and of themselves and are, thus, patentable distinct and non-obvious over the cited references in their own right. For example, it is respectfully asserted that the cited reference does not teach or suggest "wherein the public value of the SNMP manager is included in a management information base (MIB) object in the configuration file", as recited in Claim 6 (see, e.g., Stallings, p. 11, col. 2, line 66-67). Moreover, it is respectfully asserted that the cited reference does not teach or suggest "wherein the public value of the SNMP manager is initially stored in a third entity different from that associated with the SNMP manager and the SNMP agent, and the method comprises downloading the configuration from the third entity by the SNMP agent", as recited in Claim 7.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of March 22, 2006 be withdrawn, that pending claims 1-7 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicants' Deposit Account No.07-0832.

Respectfully submitted,

Patent Operations
Thomson Licensing Inc.
P.O. Box 5312
Princeton, NJ 08543-5312

By: /Guy H. Eriksen/
Guy H. Eriksen, Attorney for Applicants
Registration No.: 41,736
(609) 734-6807